I claim:

1) A security system for a computer connected to a network of computers comprising:

at least one security subsystem associated with said computer, said subsystem configured to detect attacks on said computer;

and a secure link between said security subsystem and a master system enabling data communication therebetween; wherein

said master system monitors said security subsystem through said secure link and registers information pertaining to attacks detected by said security subsystem.

2) The security system of Claim 1 further comprising a pseudo attack generator associated with said master system for generating attacks on said computer detectable by said security subsystem wherein said master system monitors said security subsystem by comparing said pseudo-attacks to said attacks detected by the security subsystem.

3) The security system of Claim 1 wherein said master system is hierarchically independent from said security subsystem.

4) The security system of Claim 1 wherein said security subsystem is hierarchically subordinate to said master system.

5) A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network, said subsystem configured to detect attacks on said network; and

a secure link between said security subsystem and a master system enabling data communication therebetween; wherein

said master system monitors said security subsystem through said secure link and registers information pertaining to the attacks detected by said security subsystem.

6) The network security system of Claim 5 wherein said master system is hierarchically independent from said security subsystem.

7) The network security system of Claim 5 wherein said security subsystem is hierarchically subordinate to said master system.

8) A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network and configured to detect and register attacks on said target network;

a secure link for data communication between said security subsystem and said master system; and

testing means associated with said master system for generating pseudo-attacks on said target network initiated by said master system and detectable by said security subsystem; wherein

said master system monitors said security subsystem through said secure link by comparing the pseudo-attacks generated by said testing means to the detected attacks registered by said security subsystem.

9) The network security system of Claim 8 wherein said master system is hierarchically independent from said security subsystem.

10) The network security system of Claim 8 wherein said security subsystem is hierarchically subordinate to said master system.

11) A method for monitoring the integrity of a security subsystem associated with a target network of computers and configured to detect attacks on said network of computers comprising:

establishing a secure link for the transfer of data between said security subsystem and a master system hierarchically independent from said security subsystem;

monitoring the status of said security subsystem through said secure link; and

registering information pertaining to the status of said security subsystem.

12) The method for monitoring the integrity of a security system of Claim 11 including the steps of:

connecting said master system and said target network separately to an open network of computers;

generating at least one pseudo-attack in said master system, said pseudo attack being detectable by said security subsystem;

generating in said master system a list of expected responses to said at least one pseudo-attack;

delivering said at least one pseudo-attack over said open network to said target network; and

comparing the response of said security subsystem to said pseudo-attack to the list of expected responses thereto.